Abstract

An embedded cryptographic system comprises at least one test plaintext/ciphertext pair P_i, C_i for which the key has been destroyed or stored at a very safe place. If at some later date, at least one apoptosis key K_i is presented to the cryptographic system which has the property that C_i is the enciphered image of P_i under K_i, then the algorithm could be broken and should not be used any more. Instead a more conservative algorithm should be used. The method for changing the ciphering by an embedded cryptographic system includes the step of checking whether at least one test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under an apoptosis key K_i and the step of switching off the used cryptographic mode in case of a positive checking result. ~~In order to enable the step of checking a protocol has to define a control stream with at least one key to be checked. The checking will be done as soon as such as control stream is received by the cryptographic system. The advantage of this solution is the fact, that there is not need for controlling respectively trusting the manufacturer or a security service. The embedded cryptographic system can receive the key or a collection of keys $\{K_i\}$ from anywhere.~~